Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Without Permission: Privacy on the Line

Joanne Pratt
Joanne H. Pratt Associates

Sue Conger

WITHOUT PERMISSION: PRIVACY ON THE LINE

Joanne H. Pratt
joannepratt@post.harvard.edu
Joanne H. Pratt Associates
3520 Routh St.
Dallas, TX 75219
214.528.6450

Sue Conger
sconger@aol.com
University of Dallas
1845 E. Northgate Dr.
Irving, TX 75062
214.850.6424

Abstract

Considerable research shows that personal information privacy has eroded over the last 30 years. Prior research, however, takes a consumer-centric view of personal information privacy, a view that leads to the conclusion that the individual is responsible for his/her own information. This research presents and defends a comprehensive personal information privacy model of extra-organizational data sharing, leakages, and transgressions of data that incorporates how data are actually passed and leaked to organizations of whom the consumer has no knowledge and over which the consumer has no control. This research presents support for the existence of the extra-organizational parties and the need for more complete comprehension of personal information privacy in business-to-consumer research. In addition, the research supports the presence of data transgressors and data invaders, identifying the magnitude of privacy violations in spite of legal and self-protection policies. The model can serve as a guide for privacy research and for social discussion and legislation to manage and regulate use of data once collected.

Keywords: Personal Information Privacy, Data Aggregator, Data Appropriator, Data Invader

Introduction

Personal privacy is a vague concept generally applied to keeping confidential anything an individual does not want known. The assumption is that we each have inalienable rights to keep private anything about us that we wish, ceding access rights in exchange for societal participation. Citizenship and employment cause us to cede right of identity, domicile location, and family arrangements. Through transactions we cede the rights to personal transaction information to aggregators who, until recently, limited their data collection and aggregation to otherwise ceded information. Recently, because of new and maturing technologies, we are unknowingly giving away much more than just identity, location, and transaction information. Aggregators and others without permission to do so, collect click-streams, phone records, Internet protocol (IP) address, personal movements, food and medicine usage, genetic makeup, DNA, and health, biological, criminal, genealogical, and financial histories. Privacy is eroding as new technologies enable this massive collection, aggregation, and sale of everything about everyone.

Data integration has led to functional, economic, and social benefits but also to abuses to individual privacy. Abuses to personal information privacy (PIP) are beginning to outweigh the benefits obtained by widespread data integration and sale. Legal data integrators are being pre-empted by para-legal and illegal entities seeking insatiable accessibility to minutia on every facet of individuals' lives.

This research first presents an expanded PIP model, defining extra-organizational data sharing entities along with the threats they pose to PIP. Then, proof of the existence and extent of threats to PIP from the fourth parties – data appropriators,

and fifth parties – data invaders is offered. The next section describes the effectiveness of current attempts to safeguard PIP by legislation and self-protection. Finally, the importance of interest in PIP issues and possible actions are presented.

An Expanded Model of Information Privacy

This section summarizes a model of information privacy that integrates extra-organizational uses of personal data provided to vendors as part of transaction processing. Each box leading to the decision calculus in Figure 1 and the arrows depicting the relationships between them represent areas in which significant research has already been conducted and incorporates the bodies of work summarized in Culnan and Armstrong (1999) and Cheung, et al. (2005).

The expanded privacy model contributes to the literature in several ways. First, it presents a model of data exchange that includes all parties: the individual holding private data; the vendor(s) to whom it is initially released; 3rd party legal data integrators, 4th party government and commercial data trespassers and 5th party data invaders. While these constructs have individually been the topic of some research, none of the research found ties the subject matter to PIP, thus presenting an incomplete view of the data relationships among organizations. Second, the model in this research integrates and enlarges separate frameworks that model privacy and online transaction processing.

Personal privacy before web maturity as modeled by Culnan and Armstrong shows the consumer disclosing information based on achieving benefits that exceed risks. The model emphasizes feedback, which enables the vendor to predict subsequent behavior such as consumer retention, defection or the attraction of new customers. Published in 1999, the model does not specifically treat online transactions; it is a privacy leverage approach. The second model (Cheung et al, 2005) treats online transactions without incorporating privacy issues. The model emphasizes the individual consumer, the product, the vendor and the environment. For each, a set of characteristics is used to model the consumer's online intention, adoption and continuance to purchase.

In contrast, the expanded model assumes the individual has made the benefit/cost calculus based on the factors that Culnan and Armstrong and Cheung et al delineate. It starts at the point the trade-off has been made and traces what happens to the data thereafter. The expanded model changes the focus from the individual to the data based on the proposition that the data has an independent existence apart from the individual, once passed to the 2nd party vendor and from the 2nd party to 3rd, 4th and 5th parties. As it is transferred, integrated, and mined, it is transformed into information that could benefit the 1st party, or as daily media coverage makes clear, subject the 1st party or others to harm.

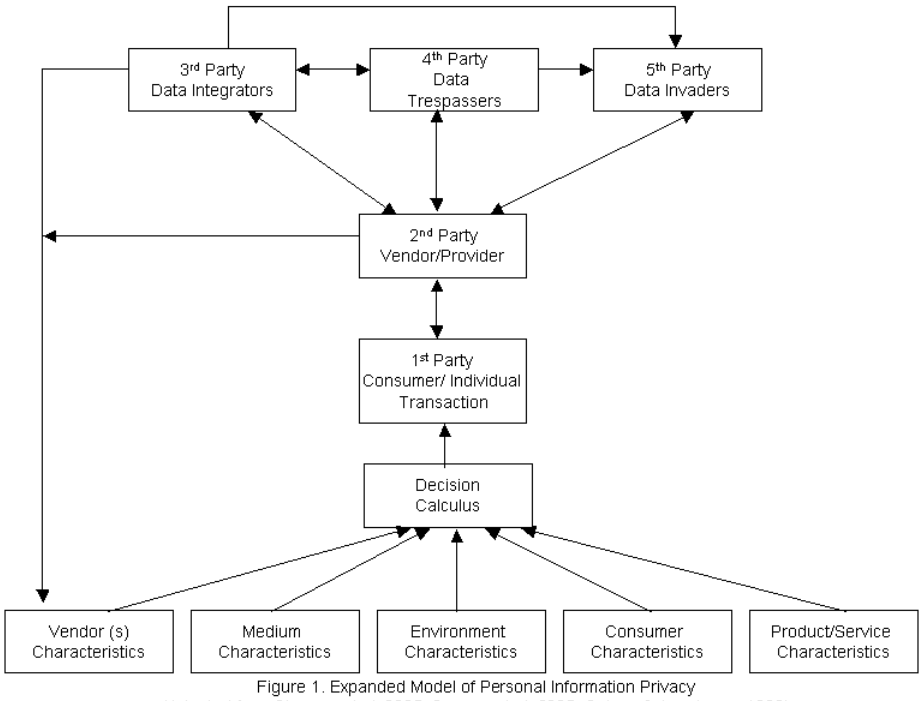

Figure 1. Expanded Model of Personal Information Privacy
(Adapted from Cheung, et al. 2005; Conger, et al. 2005; Culnan & Armstrong, 1999)

Part of the 1st party individual's decision includes what data to provide to the 2nd party vendor based on the expected life and use of that data, perceived reasonableness of the data collected, expected benefits, and expectations of corporate use of the collected data (Conger, et al.2005, McKnight, et al. 2004).

Figure 1 presents the expanded model of personal information privacy. The type of data requested leads the individual consumer to draw conclusions about the perceived reasonableness of collected data. Perceived reasonableness of data is a new construct in the decision calculus that arises from corporate use of smart technologies that can surreptitiously collect such data as click streams, personal movements, food and medicine usage, genetic markers, DNA, health, or other biological data, and criminal, genealogical, or financial history (Conger, et al. 2005, McKnight, et al 2004). The decision calculus

results in an assessment of trust and risk, to either consummate or cancel the transaction and, if consummated, which data to share and the sharing duration. It is a tradeoff in which the individual gives up privacy to gain perceived benefits.

The problem is that once the data is released, privacy cannot be restored. Data may be collected before, during, or after an actual business transaction and the data collection may be known or unknown by the consumer. Combined with other transactional and post-transactional data, this data enables, for example, the building of a consumption profile for a family that could affect their insurance or medical coverage. Consumers appear ignorant of corporate privacy policies and rely heavily on organizations that vouch for the trustworthiness of the vendor (McKnight, et al. 2004). From the consumer's perspective, stewardship is inherent in the exchange of privacy for benefits. Stewardship implies vendor protection of customers' personal information (Wernick 2006). More formal data protection was promised through the fair information practice principles, which were developed in the 1970s and 1980s and guided privacy law development throughout the world (Cate 2007). However, the ensuing directives and guidelines, whether in Europe, the Asia-Pacific region (APEC), or the U.S., are rarely invoked and often superceded, for example, by The Homeland Security Act (HSA) of 2002 and The Patriot Act of 2001 (Cate 2006, Greenleaf 2006, OECD 2003).

3rd, 4th and 5th Party Data Sharing

Third party data integrators operate legally sanctioned businesses set up in the 1960s to provide added information about their consumer bases to vending organizations. Further problems arise when 4th-party trespassers or appropriators use data without 1st-party and/or 2nd-party permission. Such partnerships might be governmental pre-emption of data (Ahrens 2006, Cauley 2006, DARPA 2002, Seffers 2000, Waller 2002) or legitimate data-sharing partners by of the 3rd-party who violate the terms of their agreements. There is no actual way for Experian, for instance, to ensure proper use since compliance is self-reported. Further, government cooption of data has come under increasing scrutiny as violating constitutional rights to privacy provisions (Zeller 2005).

The last category is 5th-party data invaders. They are unintended, unwanted, unethical and/or illegal users of vendor data. Fifth-party usage results from non-compliant employee behaviors that result in leakages or from illegal activities. Fifth-party data users obtain data without permission or knowledge of the data holders, which may be 1st, 2nd, 3rd or 4th parties (ACLU 2003, Albrecht 2004, Carlson 2006). People who steal computers and who leak names, addresses, and financial or medical information, fall into this category (Zeller 2005).

One issue in developing a new model of PIP is to provide proof of the existence of all constructs. Since the 1970's researchers have addressed issues of cyber security, (See, for example, Culnan 1993, Culnan and Bies 2003, Denning and Baugh 1999, Denning 2001, Gouldson 2001, Granville 2003). The connection of Denning, Gouldson, and Granville research to personal information privacy was unclear. The research of Culnan, Smith and others was the genesis of PIP understanding but the extent of transgressions enabled by the Internet was not yet mature so the understanding of the issues was necessarily limited (cf. Culnan 1993, Culnan and Armstrong 1999, Smith and Milberg 1996) Concerns from the early research are supported by a flood of instances of privacy violations, so recent that they are not yet documented in published research. Thus, since there has been little published research to date on extra-organizational data sharing as it relates to PIP, proof must come from press, public announcements, and other public sources. In this section, evidence supporting the role of parties beyond the vendor/provider in PIP violations is presented.

3rd Party: Data Integrators

The individual's information is shared with any number of legal data-sharing entities, that is, the 3rd-party data user who is a known external data-sharing partner such as a credit reporting company. For example, Experian legally purchases, aggregates, and sells data with 2nd-party permission. Companies such as Experian generate their revenues by matching consumer information to transaction information, profiling consumers, and reselling the expanded information. The Experians of the world are not necessarily the problem unless their use or access to data violates their legal and contractual agreements. The greater vulnerabilities arise from exchanges with their data sharing partners, the 4th and 5th parties who obtain data without permission or knowledge of their sources (Carlson 2006, Kontzer and Greenemeier 2006, Zeller 2005).

Data integrators have come under fire recently for their fulfillment of the seemingly unstoppable appetite for data for all companies about virtually every aspect of their consumers' lives.

4th Party: Data Trespassers

There are two types of 4th party data trespassers. The first type is government, illustrated by numerous failings of the US Government in this research. The second type of organizations that obtain data without the consent or knowledge or the persons on which data is collected and integrate, sell or otherwise use the data in ways unknown to the individual. In both cases, the access by the trespassers may be unknown or unsanctioned but complied with under duress by 1st and 2nd party organizations from which they obtain the data. The United States Government is one of the most prolific gatherers of data on everyone in the U. S. Provoking frequent outcries, the government pre-emption, without legal consent, constitutes trespass against U.S. citizens. Major incidents are summarized below.

In 2000, the Department of Defense (DOD) and the Federal Bureau of Investigation (FBI) sought to develop "real-time" Internet intrusion devices "without becoming intrusive" and to build an accompanying database to fight network intrusions (Seffers 2000, p. 1). In 2002, the Total Information Awareness (TIA) program was initiated through the Defense Advanced Research Projects Agency (DARPA) to collect information from Internet and phone sources to create a 360^{o} view of individuals and their inter-relationships. As of 2002, an initial version of TIA was in operation. The goal of TIA, according to DARPA's Office of Information Awareness, " was to revolutionize … U.S. ability to detect, classify, and identify foreign terrorists and decipher their plans " (Waller 2002, p. 3).

However, the TIA system was called a "disaster" likened to Orwell's 1984 and the Nazi Gestapo (Waller 2002, p. 1). The ACLU described the project as providing "government officials with the ability to snoop into all aspects of our private lives without a search warrant or proof of criminal wrongdoing" (ACLU 2002). The US Congress banned TIA funding pending a privacy assessment impact statement (Waller 2002). Although TIA as a government project disappeared, it was quietly outsourced to a data aggregator that developed and deployed the database which DOD now uses (Waller 2002).

In 2006, the National Security Agency (NSA) was found to have amassed "tens of millions" of phone call records since 2001 with "the agency's goal 'to create a database of every call ever made' within" the U.S. (Cauley 2006, p.1). Ostensibly to identify terrorists, NSA has "gained a secret window to the communication habits" of about 200 million Americans that included identifying information (Cauley 2006, p. 1). The NSA actions violated The Patriot Act of 2001 and the Foreign Intelligence Surveillance Act (FISA) of 1978 that was developed to protest U.S. citizens from illegal eavesdropping. Under FISA an 11-member court for surveillance warrants must approve all requests. A presidential executive order waived the need for a warrant (Cauley 2006).

In other government actions, The FBI and Department of Justice (DOJ), asked Google, MSN, AOL, and Yahoo to turn over current files and to retain data on surfing queries and click streams (Ahrens 2006). President Bush added a phrase to a postal reform bill that declared post office rights to open mail "as authorized by laws for foreign intelligence collection" (Memott 2007) thereby widening the collection of information about U.S. citizens without legal due process.

Thus, the U.S. Government is a prolific trespasser engaging in wholesale data collection and aggregation for purposes of tracking and monitoring all individuals in their expanding databases. When public outcries have thwarted public attempts at relentless collection of data, government agencies have outsourced or otherwise hidden the activities that have continued unabated.

The second type of data trespasser is organizations that obtain data without the knowledge of either the individuals on which the data is collected or the companies from which the data are obtained. Many organizations are legal in their operations to collect and integrate 'free' information such as sex offender records, real estate sale records and published phone records, to establish a profile that someone might buy. Some of these companies cross the line into illegality by using pretexting, which is, posing as a customer to obtain information, or tapping phone records (Associated Press 2006).

Data brokers often obtain data through deception using both legal and illegal means. One data broker declared "There are no more secrets" to the US Congress, any information can be obtained with social security numbers as easily obtained as an address (Matlin 2006, p1). During the Congressional hearings, 11 practicing brokers invoked the 5th Amendment to avoid questions about their activities (Matlin 2006).

Another form of 4th party data collection is practiced by, for instance, Aggregate Knowledge, a company that works with online vendors to develop shopping profiles through use of cookies and other online methods (Takahashi 2007). While cookies, per se, are not illegal or unethical, the tracking of movements and clickstreams, that then are aggregated with other lifestyle, psychographic and demographic information may provide more information than a consumer wants known. Therefore, opt-in programs, discussed below, should be available for such uses.

5th Party: Data Invaders

Data trespassers, such as the government and data brokers, override personal privacy concerns by justifying their action as necessary for the public good, or to prevent acts of terrorism. Data invaders have no such rationale for their transgressions.

Data invaders may be hackers, thieves or just careless employees. Denning (Denning and Baugh 1999, Denning 2001) documents criminal and terrorist activity and data vulnerability, examining, for example, the benefits and drawback of encryption to control interactions with suppliers (3rd parties), partners and customers (1st party). As the more recent literature suggests (Denning 2001), "hacktivism," defined as hacking fused with activism, has become a frequent occurrence worldwide. The Attrition organization provides an Internet database of data loss incidents (Attrition.org 2007). January and February 2007 losses include, for instance,

11,500 credit card numbers on a hacked server
160,000 personal records in a file on the Iowa Department of Education hacked web site
70,000 Vermont Agency of Human Service customers' social security numbers, names and bank information
19,000 names, and addresses and banking details from the Worcestershire County Council,
22,000 members' medical information from Kaiser Permanente
130,000 names, social security numbers and birthdates of St. Mary's Hospital patients
30,000 taxpayers' data from the North Carolina Department of Revenue
11,000 names and social security numbers posted on the City College of San Francisco web site
65,000 records posted on the East Carolina University site.

Further, Attrition cites thousands of records found in discarded boxes, in purchased used furniture and in trash behind buildings. (Attrition.org 2007, pp. 1-4)

Privacy Rights Organization, another watchdog group, reports compromised "data elements useful to identity thieves, such as social security numbers, account numbers, and driver's license numbers" (Privacy Rights Clearinghouse 2007, p 1). Their running "total number of records containing sensitive personal information involved in security breaches" reached 104,106,513 from January 10, 2005 through February 23, 2007. From February 23 through April 30, 2007, that number approximately doubles to over 200 million compromised records that would support identify theft (Privacy Rights Clearinghouse 2007, Attrition.org 2007).

From ChoicePoint's infamous identity theft in February 2004 through December 2006, there were over 500 thefts, hacks, or leakages of consumer information for which 395 organizations reported losses over 200 million individual accounts with social security information. Add to that number the organizations either not reporting or not including social security numbers would approximately double the number of transgressions. If all lost information was reported, whether or not social security information were included, virtually every person in the United States has had their information compromised at increasing privacy and dollar cost. "The FBI estimates that [cybercrime] cost the U.S. more than $67 billion last year" (McMillan 2006, p. 1). Further, estimates of the cost of poor privacy control on the part of organizations that are hacked, leaked, or otherwise compromised is $90 to $305 per record (Gaudin 2007).

Safeguarding Privacy

Protection may take the form of public policy carried out by federal and state legislation or it may occur by individual PIP management, for example, by response to "opt-out" provisions offered by vendors as their own self-protection. The Privacy Act attempts to balance the government's need for information about individuals against protection of their privacy. Enacted in 1974 to curb illegal surveillance, policy emphasis has shifted from issues raised during Watergate to life threatening concerns of further terrorism after 9/11/2001. The Patriot Act of 2001 justified expanded surveillance at the cost of individual privacy. The Patriot Act is a fundamental basis of privacy law.

Legal Protection

In response to "technological changes in computers, digitized networks, and the creation of new information products," privacy law attempts to protect "against unauthorized use of the collected information and government access to private records." (BBBBOnLine, Inc. and the Council of Better Business Bureaus, Inc. No date p. 1). Thirty-four states have notification laws (Wernick 2006). Typically, the state laws cover combinations of an individual's name with unencrypted data items ranging from social security number to DNA profile. However, statutes exclude information available to the public in federal, state or local records. California created a State Office of Privacy Protection in 2000 and has enacted laws that protect citizens' privacy across many facets of their lives. State regulations, for example, include limits to retrieval of information from automobile "black boxes" (California Department of Consumer Affairs 2006, p. 1) disclosure of personal information on drivers' licenses, protection of confidentiality of library circulation records, and bans on embedding social

security numbers on "a card or document using a bar code, chip, magnetic strip…" (p. 3). The State also defines a "specific crime of identity theft" (p. 4).

Similarly, Federal privacy laws afford privacy protection of cable subscriber information, drivers' license and motor vehicle registration records, "prohibits persons from tampering with computers or accessing certain computerized records without authorization" require protection of medical records and so on (BBBBOnLine, Inc. and the Council of Better Business Bureaus, Inc. No date p. 3).

Legal recourse is also available under some conditions that are more abstract than, for example, protecting disclosure of specified transactions. To enact a transaction, the individual discloses personal information based on an assumption of trust in a specific relationship with the recipient of the data. A *tort of breach of confidentiality* offers legal recourse when that trust is broken (Solove 2006).

The problem is that although many statutes, both Federal and State, address privacy protection in many facets of individuals' lives, the government has the power to "trump" those laws via, for instance, The Homeland Security Act (HSA) of 2002. Once data integration occurs in the context of a short-term emergency, such as ferreting out terrorists, individual privacy cannot be restored. In fact, known transgressions of HSA by the government have led to records of innocent parties being propagated through generations of federal databases of suspected terrorists (Gellman 2005).

Individual PIP Management

Two arguments against government regulation of PIP are that individuals should manage their own privacy or that vendors should be held responsible, since it is in their own interest to avoid potential liabilities and costs (Wernick 2006). However, with invisible, unknown means of surveillance and tracking, individuals are unable to manage their information. For instance, in one demonstration, an individual was tracked by means of over 120 readings of radio-frequency identification (RFID) and smart card chips, the global positioning system (GPS) in the cell phone and other methods in a single day to show how tracking becomes possible. Further, with legal relationships (and illegal ones), far removed from the original transacting vendor, even the vendors do not know where their data goes once it leaves their confines. Opting into and out of selling programs has been touted as an answer to individual PIP management. However, even that option is not without its issues as is described in this section.

Opt-Out

In general, opt-out is at the discretion of the vendor with each vendor developing its own rules. Opting out of a database registry may be as simple as emailing a request (Aristotle 2007) or validating one's identity, or as complex as proving one is at risk of bodily harm. Three examples suggest the range of privacy agreements: The Ameridex Information Systems requires the individual to "…email…the following information…formatted as shown…: first-name, middle initial, last-name, city, state, year-of-birth, month-of-birth, day-of-birth…." and cautions "Note: We cannot block retrievals of listed telephone numbers. You must notify your telephone company to delist your telephone number" (Ameridex 2007, p. 1).

Intellius spells out the difficulty of removing personal information that has been captured in public databases: "If you have a compelling privacy or security issue, you may wish to contact the official custodians of those public records that contain sensitive information about you, such as your county's land records office, to determine how to remove your information from the public record (The process of having public records sealed typically requires a court order.)" (Intellius 2006).

Opt-out requests to the LexisNexis web site receive the explanation "To opt out, you must provide LexisNexis with an explanation of the reason…for the request, including: you are a law enforcement officer…[state] that your position exposes you to a threat of death or serious bodily harm; or if you are a victim of identity theft…submit an Identity Theft Affidavit…or if you are at risk of physical harm and are not involved in law enforcement…submit a…protective court order…" (LexisNexis 2005).

Opt-In

Opt-in provisions typically pertain to information that the individual supplies for inclusion in a database. The Genealogy.com site specifies that "Once you contribute content to the World Family Tree…you may not edit or remove such content…such content that you submit…to Virtual Cemetery, may become part of an online archive…database that may be reproduced by Genealogy.com in any format…for distribution, sale, or any other purpose" (Genealogy.com 2004).

A seeming third approach are the data gatherers who offer neither an opt out or opt-in provision such as DocuSearch: "You cannot opt out [or in] …Public records, by law, must be available…to anyone who requests them…our service is used by investigators, law enforcement agents and lawyers … to locate criminal, debtors and other bad actors. Accordingly, it would defeat the purpose of our service if we gave these types of individuals the ability to opt out of being found" (DocuSearch 2007). Therefore, the consumer has opted in, whether voluntarily or not.

Research on opt-in systems show that they are expensive to administer and do not solve the privacy issues involved (Cate, 2007). As the model presented in this research clarifies, the reason is because the data takes on its own life once given to a vendor.

Discussion

PIP is increasingly important in a world of technologies that support tracking, monitoring, and the ability to collect information about every facet of private life. In this world, public safety must be balanced against the need for personal privacy. Problems arise when consumers unknowingly become targets of data collection of which they are not aware. By opting for the benefits of data sharing in a transaction, unknown risks are undertaken that unknown data will be collected, sold or shared, and become part of the public record about the individual. The issues of who can or should control data life, integration and use need further discussion and resolution. The resolution may be a long time in coming as it will likely require some extent of social and cultural change. Even in societies, such as European Union, that place a high premium on personal privacy, PIP erosion remains an issue. In the mean time, knowledge that data has its own life should be better understood to inform individual decisions.

Summary

This research presents an expanded privacy model, incorporating extra-organizational data sharing, leakages, and transgressions of data, thus clarifying inter-relationships between known and unknown parties to individual transactions and highlighting that once given, data takes on a life of its own. The model highlights the need for attention to vendor data collection and sharing practices to safeguard private information. Examples of 4th party government trespass and 5th party data invasion support the existence of these parties and emphasize this growing problem. Data integration and appropriation generate risks to privacy, which have become pervasive throughout society. Data invasion has become an everyday occurrence. With these changes to PIP, the expanded privacy model shows that attention to all parties accessing information is needed to accurately comprehend the decision calculus process that leads to the sharing of personal information with vendors. Once the data are provided, consumers should expect that their data might be shared or sold with any number of other organizations, including organizations that have negative intentions.

References

ACLU, "RFID position statement of consumer privacy and civil liberties organizations," American Civil Liberties Union (ACLU), November 30, 2003.

ACLU, "Defend your right to privacy," American Civil Liberties Union of Southern California, November 21, 2002. http://ga1.org/aclu_sc_action/alert-description.html?alert_id=4132.

Ahrens, Frank, "Government, Internet firms in talks over browsing data," *Washington Post*, June 3, 2006, p D3.

Albrecht, Katherine," Supermarket Cards: The Tip of the Retail Surveillance Iceberg," Denver university Law Review, 79(4, 15), 534-554, 2002.

Ameridex, "Privacy Statement," Ameridex Information Systems, February 27, 2007. Downloaded from http://ameridex.com/privacy.html.

Aristotle, “Privacy Policy: Privacy Statement for www. Aristotle.com.” 2007. Downloaded from http://www.aristotle.com/privacy_policy.htm

Associated Press, "AT&T sues brokers over customer data," MSNBC.Com and Associated Press, August 23, 2006.

Attrition.org, “Attrition.org, Data Loss Archive and Database (DLDOS),” March 3, 2007. Downloaded from http://attrition.org/dataloss/

Attrition.org, “Data Loss: Why We Do This,” February 20, 2007. Downloaded from http://attrition.org/dataloss/why.html.

BBBBOnLine, Inc. and the Council of Better Business Bureaus, Inc. A Review of Federal and State Privacy Laws. No date. Downloaded from http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf, March 2007.

California Department of Consumer Affairs. “Privacy Laws,” Office of Privacy Protection, February 14, 2006. Downloaded from http://www.privacy.ca.gov/lawenforcement/laws.htm California laws

Carlson, Caron, "Unauthorized sale of phone records on the rise, eWeek, February 1, 2006.

Cate, F. H., "The Failure of Fair Information Practice Principles," in Jane K. Winn, ed., Consumer Protection in the Age of the 'Information Economy,' Ashgate, 2006, p. 341.

Cate, F. H., and Staten, M. E., “Protecting Privacy in the New Millennium: The Fallacy of Opt-in,” National Retail Foundation (2000).

Cauley, Leslie, "NSA has massive database of Americans' phone calls," *USA Today*, May 11, 2006, Downloaded from http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

Cauley, L., "AT&T sues 'data brokers' in access case," *USA Today*, August 23, 2006.

Cheung, Christy MK, Gloria WW Chan, and Moez Limayem, "A Critical Review of Online Consumer Behavior: Empirical Research," Journal of Electronic Commerce in Organizations, Oct-Dec, 2005, 3(4), 1-19.

Conger, Sue, Richard O. Mason, Florence Mason, Joanne H. Pratt, "The Connected Home: Poison or Paradise," Proceedings of Academy of Management Meeting, Honolulu, HI, August, 2005.

Culnan, M.J., "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," MIS Quarterly (17:3), 1993, pp. 341-363.

Culnan, M.J., and Armstrong, P. K., “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation,” Organization Science, (10:1), January 1999, pp.104-115.

Culnan, M.J., and R.J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations," Journal of Social Issues (59:2), 2003, pp. 323-342.

DARPA, "DarpaTech 2002 Symposium: Transforming fantasy," Defense Applied Research Projects Agency, 2002.

Denning, D. E., and Baugh, W. E. Jr., “Hiding Crimes in Cyberspace,” Information, Communication and Society (2:3), September 1999, pp. 251-276.

Denning, D., “Cyberwarriors: Activists and Terrorists Turn to Cyberspace,” Harvard International Review, (23:2), Summer 2001, pp. 70-75.

Denning, D., “To Tap or Not,” and Comments, Communications of the ACM (36:3), March 1993, pp. 24-42.

DocuSearch, “Privacy Statements: Opting Out,” Downloaded March 2007 from http://docusearch.com/privacy.html

Gaudin, S., "Security breaches Cost $90 to $305 Per Lost Record" *Information Week*, April 11, 2007. Downloaded from http://www.informationweek.com/shared/printableArticle.jhtml?articleID=199000222

Gellman, B., "The FBI's Secret Scrutiny," *The Washington Post*, November 6, 2005, Pg A01.

Geneology.com “Privacy Statement: Home Pages, Family Trees, Virtual Cemetery and the World Family Tree,” July 21, 2004. Downloaded from www.genealogy.com/privacy.html

Gouldson, T., “Hackers and Crackers Bedevil Business World,” Computing Canada; July 27, 2001; 27, 16; p. 13.

Granville, J., Review Article on Global Governance, Global Society (17:1), January 2003, pp. 89-97.

Greenleaf, G., “APEC’s Privacy Framework sets a new low standard for the Asia-Pacific” in M. Richardson and A. Kenyon (eds.), New Dimensions in Privacy Law: International and Comparative Perspectives, Cambridge: Cambridge University Press, 2006.

Intellius. **“**Welcome to the Intelius Privacy FAQ: How can I remove my information from the Intelius public records databases?” February 16, 2006. Downloaded from http://find.intelius.com/privacy-faq.php#8

Kontzer, Tony and Larry Greenemeier, "Sad State of Data Security," Information Week, January 2, 2006, 19-22.

LexisNexis. “Data Privacy Policy” Opt-Out Requests,” March 29, 2005. Downloaded from http://www.lexisnexis.com/terms/privacy/data/remove.asp

Matlin, C., "'Data Broker' Reveals ID Theft Secrets," ABC News, June 21, 2006. Downloaded from http://abcnews.go.com/US/print?id=2104646

McCullagh, D., “Report: FBI's Snooping Did Not Follow Rules,” CNET News.com, March 9, 2007.

McKnight, Harrison, Vivek Choudhury, Charles Kacmar, "Dispositional and Distrust Distinctions in Predicting High and Low Risk Internet Expert Advice Site Perceptions," E-Service Journal, Winter, 2004 3(2), 35-59.

McMillan, R. [08-09-06] - Robert – “Defcon: Cybercriminals taking cues from Mafia, says FBI, “Computerworld Security August 6, 2006. Downloaded from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_hacking&articleId=9002230&taxonomyId=82

Memott, Mark. "Bush says feds can open mail without warrants," USA Today, January 4, 2007, http://blogs.usatoday.com/ondeadline/2007/01/bush_says_feds_.html .

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 2000.

OECD, Privacy Online: Policy and Practical Guidance, OECD, 2003.

Privacy Rights Clearinghouse, “A Chronology of Data Breaches,” February 24, 2007. Downloaded from http://www.privacyrights.org/ar/ChronDataBreaches.htm

Seffers, George, "DOD database to fight cybercrime," *Federal Computer Week*, November 2, 2000, Downloaded from http://www.fcw.com/fcw/articles/2000/1030/web-data-11-02-00.asp

Smith, H. J., and Milberg, S J, “Information Privacy: Measuring Individuals' Concerns about Organizational Practices,” MIS Quarterly (20:2), June 1996, pp.167-196.

Solove, Daniel J., “A Taxonomy of Privacy,” University of Pennsylvania Law Review, 154(3) (January, 2006), pp. 477-560.

Takahashi, D., "Demo: Aggregate Knowledge Knows What You Want To Buy," *San Jose Mercury News*, January 30, 2007. Downloaded from www.mercextra.com/blogs/takahashi/2007/01/30/demo-aggregate-knowledge-knows-what-you-want-to-buy/

Waller, J. Michael, "Fears mount over 'total' spy system: civil libertarians and privacy-rights advocates are fearful of a new federal database aimed at storing vast quantities of personal data to identify terrorist threats – Nation: homeland security," *Insight Magazine*, December 24, 2002, Downloaded from http://www.findarticles.com/p/articles/mi_m1571/is_1_19/ai_95914215

Wernick, Alan S., “Data Theft and State Law,” Journal of AHIMA, December, 2006, pp. 40-44.

Zeller, Tom, Jr., "Another Data Broker Reports a Breach," *The New York Times*, March 10, 2005.

Zeller, Tom, Jr., "Personal Data for the Taking," *The New York Times*, May 18, 2005.